

REMARKS

Applicant has carefully reviewed the arguments presented in the Office Action and respectfully requests entry of the amendment and reconsideration of the application, as amended, in view of the remarks presented below.

Claim 291 has been amended. Claims 1-114, 122-229, 233, 235, and 237-285 have been canceled. Thus claims 115-121, 230-232, 234, 236 and 237-297 remain pending in the application.

Claim 291 was amended to correct an inadvertent typographical error. No new matter was added by way of this amendment.

Claims 115-121, 230-232, 236 and 286-297 have been rejected under 35 U.S.C. § 103(a), as being unpatentable over Barkan (International Publication No. WO 98/17042) in view of Zabetian, U.S. Patent No. 6,327,656. Applicant respectfully traverses these rejections.

The crux of the Examiner's rejections apparently is his belief that Barkan discloses the step of "storing at the server at least a portion of a dialog generated during the transmission of the message between the server and the destination address [see p.23-24, steps j-h, p.29-30, 31-32, 34]." Office Action at 18, ll. 4-6. Applicant respectfully disagrees with the Examiner.

First, it is axiomatic that the entire claim be examined in its entirety. This means that all the words of an element or limitation must be considered when evaluating the teachings of a prior art reference. In this application, independent claim 115 recited the step of: "storing at the server at least a portion of a mail transport protocol dialog generated during the transmission of the message between the server and the destination address." Independent claim 230 contains similar language: "creating an electronic attachment at the second server including the identity and address of the sender and the identity and address of the second server and the identity and address of the destination server and at least a portion of a mail transport protocol dialog generated during the transmission of the message between the second server and the destination server."

Contrary to the Examiner's assertion, Barkan neither teaches nor suggests storing at least a portion of a mail transport protocol or creating an electronic attachment including at least a portion of a mail transport protocol dialog. The pages in Barkan cited by the Examiner do not contain the words "mail transport protocol dialog." In fact, they do not contain the word "dialog" at all. Applicants believe that the Examiner has used impermissible hindsight reconstruction to obtain Applicant's claimed language.

A dialog, as that term is understood by one skilled in the relevant art, is a list of commands and responses exchanged between an outgoing server and a destination address or server to transmit a message. *See, e.g., "Network Design Manual: Storing and Forwarding With SMTP and Message Transfer Agents,"* attached hereto as Appendix A. The dialog is separate from the transmission of the message itself. The commands and responses are part of the process of actually transmitting the message. As recited by Applicant in claims 115 and 230, Applicant either stores at least a portion of the commands and responses exchanged between servers or creates an attachment with at least a portion of those commands. Barkan simply does not teach or suggest either of these steps.

Barkan discloses an email system that uses various encryption methods and public and private keys. Information is passed back and forth between senders and recipients. However, nowhere does Barkan teach or suggest storing at least a portion of a mail transport protocol dialog, that is, the commands and responses that are exchanged between the server and destination address as part of the mail transport process generated during transmission of the message between the server and destination address for subsequent proof of the message and the delivery of the message by the server to the destination address, as is claimed in amended claim 115.

For example, Barkan, at page 23-24, in step d. teaches "a fourth message including a notice that an E-mail message was sent to a second user, the CRC or hash of the message, the identification of the intermediary 71 and the serial number or message identification." There is no teaching of storing at least part of a mail transport protocol dialog. Barkan clearly states that the LRM transmission program prepares a notification that an E-mail message was sent. This is

different from storing at least part of a mail transport protocol dialog which is an exchange of commands between sending and receiving servers.

In step e., Barkan merely teaches sending various messages to various users, with no mention of storing at least part of a mail transport protocol dialog, or using at least a portion of a mail transport protocol dialog as contents of the message. For example, step discloses a third message and a second message. Both of these messages are prepared by the LRM program. In step f., Barkan teaches presenting a second user with information relating to a received message, but there is no mention of storing at least part of a mail transport protocol dialog. Similarly, step g. discloses encrypting a fourth message with a private key of a second user to create a fifth message, the fifth message being a receipt signed by the second user with his key, including the message identification and the CRC or hash relating to the contents of the message. There is no disclosure of storing at least a portion of a mail transport protocol dialog, or using at least a portion of a mail transport protocol dialog as contents of the message. The same applies to the disclosure of step h.

Similarly, Barkan at pages 29-30, 31-32 and 34 fails to disclose or even suggest storing at least part of a mail transport protocol dialog or using at least a portion of a mail transport protocol dialog as contents of the message. Barkan teaches a system using multiple messages and public and private key encryption, a complicated system that is simply not required using Applicant's claimed invention. Moreover, using Applicant's invention of amended claim 115 provides proof of the message, and that the message was delivered by recording the mail transport protocol dialog generated during transmission of the message, thus avoiding all of the additional messages and complicated encryption technology of Barkan.

Moreover, while Zabetian does teach using conventional network communication protocols such as SMTP and the like to transmit electronic documents, Zabetian does not teach or suggest storing at least a portion of a mail transport protocol dialog generated by those protocols during transmission of the document. Using a protocol to communicate documents in a network is not the same as storing at least a portion of the communications between servers and destinations that occur as the result of using that protocol. While persons skilled in the art would have been aware of the flow of information that is part of the protocol, Applicant alone

recognized the importance of storing the dialog that occurs between a server and destination address that is generated when using a mail transport protocol such as SMTP for later use in proof of the message and proof of the delivery of the message. For these reasons, Applicant submits that claim 115 is patentable over the cited art and respectfully requests that the rejection be withdrawn and that claim 115 and its dependent claims, be allowed. (Emphasis added).

Similar to claim 115, claim 230 recites creating an electronic attachment at a second server including the identity and address of the sender and the identity and address of the second server and the identity and address of the destination server and at least a portion of a mail transport protocol dialog generated during the transmission of the message between the second sever and destination server. As described with reference to claim 115, neither Barkan nor Zabetian, taken alone or in combination, teach or even suggest the novel method of claim 230. Further, none of the art, alone or in combination, teach or suggest creating an electronic attachment including at least a portion of a mail transport protocol dialog before any authentication of the message, as is claimed in claim 230. Accordingly, Applicant submits that claim 230 is patentable over the cited art and requests that the rejection be withdrawn and that claim 230 and the claims dependent therefrom be allowed.

In summary, while Barkan does teach a system of multiple messages transmitted between various servers, none of those messages are formed using at least a portion of a mail transport protocol dialog, that is, none of Barkan's messages, keys or other encryption devices store or use any portion of the actual mail transport protocol dialog exchanged by the servers disclosed by Barkan. The mail transport protocol dialog recited by Applicant in claims 115 and 230 is not part of any message that is transmitted in Barkan. Moreover, while Zabetian does teach using an SMTP protocol, Zabetian fails to teach or even suggest storing or using any portion of the commands and responses exchanged between servers using the SMTP protocol to transmit a message. Accordingly, Applicant respectfully submits that claims 115 and 230, and all of the claims dependent therefrom are patentable over the art of record, taken alone or in combination, and asks that the rejections be withdrawn and that those claims be allowed.

CONCLUSION

Applicant has carefully reviewed the arguments presented in the Office Action and respectfully requests reconsideration of the claims in view of the remarks presented. In light of the above amendments and remarks, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Should the Examiner have any questions concerning the above amendments and arguments, or any suggestions to obtain allowance, Applicant requests that the Examiner contact Applicant's attorney, John K. Fitzgerald, at 310-824-5555.

The Commissioner is authorized to credit any overpayment or charge any additional fees in this matter to our Deposit Account No. 06-2425.

Date: May 13, 2010

Respectfully submitted,

FULWIDER PATTON LLP

/john k. fitzgerald/
John K. Fitzgerald
Reg. No. 38,881

JKF:vmm

Howard Hughes Center
6060 Civic Center Drive, Tenth Floor
Los Angeles, CA 90045
Telephone: (310) 824-5555
Facsimile: (310) 824-9696
Customer No. 24201
401161.1

APPENDIX A

Comprehensive thought leadership for executives, IT professionals and developers. Topics include: the ROI, cost and economics of on-demand computing; Migration strategies to move from on-premise to cloud-based IT; Vertical cloud specialization, tailoring features and architectures to specific applications, industries, and customer ecosystems

[More Events »](#)

Vendor Newsfeed

[ARM Accelerates Data Replication With New Isilon IQ 10000X-SSD](#)

[EMC Helps Define Information Governance for Microsoft Exchange 2010](#)

[SonicWALL Expands Deep Packet Protection With SSL Inspection for Midsized and Large Businesses](#)

[Cisco and TANDBERG Provide Technology Roadmap Update Prior to Transaction Close](#)

[Isilon Turbo-Charges Scale-out NAS With Solid State Drives](#)

[Veeva Connection Broker 6.3 Makes Enterprise Desktop Virtualization Easier To Deploy Through Greater Flexibility And Simplified Management](#)

[More Vendor Newsfeed »](#)

Subscribe to Newsletter

- Keep up with all of the latest news and analysis on the fast-moving IT industry with Network Computing newsletters.

[Sign Up](#)

Network Design Manual

Storing and Forwarding With SMTP And Message Transfer Agents

Describing the Basic SMTP Dialogs

As a user, you are undoubtedly familiar with MUAs and what they do for you, but you may be unsure as to how they work. When you create a mail message using an MTA. As you create the message, you provide content as well as address information and your own identity. When you finally send the message, the MUA opens a TCP connection with your outgoing MTA.

Your outgoing MTA server communicates with your MUA using SMTP. The MTA listens for a TCP connection on port 25. After your MUA connects, it starts a command dialog according to the SMTP specification. Indicating the sender of the message rather than the targeted recipient accomplishes this. (At this point, the MTA can deny access based on the identity of the user sending the message.)

By employing a set of rules based on domain names or IP addresses, messages can be filtered and not relayed any further. This prevents unauthorized users, such as hackers, from using your MTA as a free on-ramp to the Internet. Any size installation should definitely have this ability. If you do not, you may be subject to intolerable amounts of spam and junk mail.

After the identity of the client is verified, the client machine tells the MTA the destination address or addresses. The MTA can then respond to each address and either deny or allow transmission to that address. If the address is not local, the MTA will respond with an appropriate error code and either forward the mail itself or allow the client to contact the destination MTA.

Here is a typical SMTP dialog between a client and an MTA:

MTA: 220 TEST.NWC.COM Simple Mail Transfer Service Ready

MUA: MAIL FROM:

MTA: 250 Sender OK

MUA: RCPT TO:

MTA: 250 Recipient OK

MUA: DATA

MUA: 354 Enter mail input; end with

.

MUA: This is a test message.

MUA: I will end this message with a period all by itself.

MUA: .

MTA: 250 OK

MUA: QUIT

MTA: 221 TEST.NWC.COM closing connection.

If a client machine wanted to send this message to more than one person, there would simply be more than one RCPT command, indicating additional destination addresses. Similarly, more than one message can be sent per SMTP dialog. To send additional messages, the MUA would not issue the QUIT command until it was done sending all of its mail. For each message, a line with nothing but a period and a carriage return indicates the end of the message body.

When a mail message is relayed from one MTA to another, the MAIL command also indicates the originating host. The following example shows the SMTP dialog between a relay host (TEST.NWC.COM) and the destination host (OZ.COM) that is relaying a message from FRED@SOMEWHERE.COM to WIZARD@OZ.COM.

```
MTA1: 220 oz.com Simple Mail Transfer Service Ready
```

```
MTA2: HELO test.nwc.com
MTA1: 250 oz.com
```

```
MTA2: MAIL FROM:
<
@test.nwc.com:fred@somewher
e.com>
MTA1: 250 OK
```

```
MTA2: RCPT TO:
MTA1: 250 OK
```

```
MTA2: DATA
...
MTA2: QUIT
```

To experience an SMTP dialog, any user can telnet into their SMTP server on port 25. You will find prompts similar to what we have described above. Take some time to become familiar with SMTP and how it works. In the event there is a problem with sending or receiving mail, knowing how SMTP works and what commands are necessary can oftentimes reveal the source of the problem with minimal effort.

Depending on what MTA you are using, you will have different security options. Sendmail, for example, allows you to restrict SMTP connections based on host name, domain name and IP addresses. Other packages allow further restriction based on recipient or destination address. Some MTAs go even further to screen the data portion of the mail message. For example, NTMail from Internet-Shopper can screen message content for forbidden words, preventing unsuitable material from entering your users' mailboxes. Available security options should be on your list of MTA features when considering your MTA options. Consider e-mail a security risk, and take steps now to prevent headaches later.

[← Previous Page](#)[Next Page →](#)[Print This Page](#)[E-mail this URL](#)

Best of the Web

Data deduplication: Declawing the clones

Data deduplication is emerging as a critically important new arrow in the storage administrator's quiver to answer hard questions about the increasing problem in storage growth costs.

[Quick Read](#)

Compression, Encryption, Deduplication, and Replication: Strange Bedfellows

One of the great ironies of storage technology is the inverse relationship between efficiency and security: Adding performance or reducing storage requirements almost always results in reducing the confidentiality, integrity, or availability of a system.

[Quick Read](#)

WAN Optimization Whitelists and Blacklists

Optimization is a fantastic way of saving money and creating really happy customers at the same time, but it doesn't work flawlessly for all applications.